TECLAB

INSTITUTO TÉCNICO SUPERIOR

ACTIVIDAD PRÁCTICA INTEGRADORA · MÓDULO 3

Riesgos, auditoría informática y DevOps en la nube

Identificación de riesgos en la arquitectura cloud de Tech Consulting, funcionalidades de la auditoría informática y beneficios de integrar la cultura DevOps con la nube.

ASIGNATURA	Seguridad en la Nube y Protección de Datos
CARRERA	Tecnicatura Superior en Seguridad Informática
ACTIVIDAD	Actividad 3 – Virtualización y contenedores
ESTUDIANTE	Juan Manuel Silva
LUGAR Y FECHA	Las Breñas, Chaco, Argentina · Octubre de 2026

Índice

Introducción 3

1. Riesgos en las arquitecturas cloud 4

1.1 Superficie de riesgo de la arquitectura propuesta 4

1.2 Riesgos de virtualización, segmentación y aislamiento 4

1.3 Riesgo de malware 5

1.4 Puntos únicos de fallo y alta disponibilidad 5

1.5 Riesgos de contenedores y de infraestructura mutable 6

1.6 Matriz consolidada de riesgos 6

2. Funcionalidades de la auditoría informática 8

2.1 Concepto y beneficios 8

2.2 Tipos de auditoría aplicados al caso 9

2.3 Registros de auditoría en la nube 9

2.4 Funcionalidades y proceso de auditoría 10

3. Beneficios de la integración DevOps + Cloud 11

3.1 Qué es y qué no es DevOps 11

3.2 Pipeline CI/CD propuesto 11

3.3 Contenedores, orquestación e infraestructura inmutable 12

3.4 Beneficios para Tech Consulting 13

3.5 Cómo medir los beneficios 14

4. Conclusiones 15

5. Referencias bibliográficas 16

Introducción

En las actividades anteriores se planteó la problemática de **Tech Consulting**, se definieron los objetivos de su migración a Amazon Web Services (AWS) y se diseñó la arquitectura de infraestructura: una VPC con tres capas de subredes en dos zonas de disponibilidad, cómputo con EC2 y contenedores en ECS Fargate, almacenamiento en Amazon S3 y bases SQL Server gestionadas en Amazon RDS.

Este trabajo analiza esa arquitectura desde tres miradas complementarias. Primero, **identifica los riesgos** a los que está expuesta, tomando como ejes los contenidos del Módulo 3: virtualización e hipervisores, segmentación y aislamiento, *malware*, alta disponibilidad, contenedores e infraestructura inmutable. Segundo, define las **funcionalidades de la auditoría informática** que permitirán verificar que los controles funcionan. Tercero, expone los **beneficios de integrar la cultura DevOps con la nube** como forma de construir y operar la plataforma de manera rápida, repetible y segura.

> **ALCANCE DEL TRABAJO**
>
> La propuesta es **conceptual**: no se ejecutan auditorías ni se despliegan herramientas, y no se incurre en costos. Las probabilidades e impactos de la matriz de riesgos son estimaciones cualitativas que deberían validarse con información real de la organización.

1 Riesgos en las arquitecturas cloud

1.1 Superficie de riesgo de la arquitectura propuesta

Toda la arquitectura se apoya en la **virtualización**: AWS ejecuta las instancias sobre un hipervisor de tipo 1 (nativo), que corre directamente sobre el hardware y aísla las máquinas virtuales de distintos clientes. Por encima de esa base, cada capa agrega su propia superficie de ataque. Bajo el modelo de responsabilidad compartida, la seguridad del hipervisor y del hardware corresponde a AWS, mientras que todo lo que Tech Consulting configura —red, identidades, sistemas operativos, contenedores y datos— es responsabilidad de la empresa.

Tabla 1. Capas de la arquitectura y responsable de su seguridad

Capa	Componentes	Responsable	Riesgo principal
Física y virtualización	Centros de datos, servidores, hipervisor (AWS Nitro)	AWS	Escape de máquina virtual o falla del hipervisor.
Red	VPC, subredes, rutas, security groups, VPN	Tech Consulting	Reglas demasiado permisivas y falta de segmentación.
Identidades	Cuenta raíz, usuarios, roles y políticas IAM	Tech Consulting	Credenciales robadas y privilegios excesivos.
Cómputo	Instancias EC2, contenedores en ECS Fargate	Compartido	*Malware*, imágenes vulnerables y falta de parches.
Datos	Amazon S3, RDS for SQL Server, volúmenes EBS	Tech Consulting	Exposición pública, pérdida o cifrado por *ransomware*.
Operación	Despliegues, cambios, registros	Tech Consulting	Cambios manuales no controlados y falta de trazabilidad.

Fuente: elaboración propia.

1.2 Riesgos de virtualización, segmentación y aislamiento

La **segmentación de red** divide una red en subredes que funcionan como redes propias, lo que permite definir políticas detalladas para controlar el tráfico entre ellas. Segmentar implica aislar: si un segmento se ve comprometido, el atacante no debería poder moverse libremente hacia los demás.

- **Movimiento lateral:** si las capas de aplicación y datos compartieran reglas amplias, una instancia comprometida podría alcanzar directamente las bases de datos. *Control:* las tres capas de subredes del TP2 y los *security groups* encadenados (cada capa sólo acepta tráfico de la anterior), sumados a Network ACL como segunda barrera.
- **Exposición accidental:** abrir puertos de administración (SSH/RDP) o asignar IP públicas a servidores internos. *Control:* sin IP públicas en subredes privadas, acceso administrativo mediante Session

Manager y reglas de AWS Config que alertan ante cualquier puerto abierto a Internet.

- **Firewall perimetral insuficiente:** los *firewalls* filtran el tráfico entrante y saliente según reglas, advierten intentos de conexión y bloquean aplicaciones riesgosas. *Control:* AWS WAF delante del balanceador y AWS Network Firewall para inspeccionar el tráfico de salida.
- **Escape de máquina virtual:** una vulnerabilidad del hipervisor permitiría a una máquina virtual acceder a otras del mismo host. Es un riesgo de baja probabilidad que el modelo de responsabilidad compartida **transfiere** al proveedor.

1.3 Riesgo de malware

El *malware* es un programa que se instala sin el conocimiento del propietario para robar información o tomar el control del sistema. En la nube no desaparece: cambia de vector. La siguiente tabla relaciona los tipos vistos en el módulo con el escenario de Tech Consulting.

Tabla 2. Tipos de malware y su impacto en el caso

Tipo	Vector probable en Tech Consulting	Controles propuestos
Virus	Planillas Excel con macros maliciosas cargadas al data lake o compartidas entre áreas.	Escaneo de archivos en la carga a S3; bloqueo de macros en los equipos de usuario; antivirus en estaciones de trabajo.
Gusano	Propagación desde un equipo on-premise infectado hacia la VPC a través de la VPN.	Segmentación, reglas mínimas en la VPN y detección de tráfico anómalo con GuardDuty y VPC Flow Logs.
Troyano	Dependencias o imágenes de contenedor aparentemente legítimas que esconden código malicioso.	Sólo imágenes de repositorios confiables, escaneo en Amazon ECR y Amazon Inspector.
Spyware	Robo de credenciales de consola desde equipos de los administradores.	MFA obligatorio, sesiones cortas y alertas por inicios de sesión inusuales.
Ransomware	Cifrado de bases y archivos, y borrado de las copias para forzar un pago.	Copias con AWS Backup en una cuenta separada, bóveda inmutable (*Vault Lock*), S3 Object Lock y versionado.

Fuente: elaboración propia con base en "¿Qué es un malware?" (2021).

Las medidas básicas del módulo —antivirus, copias de seguridad regulares, actualización de parches, control riguroso de accesos y concientización del personal— siguen vigentes; en la nube se complementan con detección gestionada (Amazon GuardDuty, incluida su protección contra *malware* en EC2 y S3) y con copias que el atacante no pueda alterar.

1.4 Puntos únicos de fallo y alta disponibilidad

La regla básica de la alta disponibilidad (HA) es la replicación de elementos. Un **punto único de fallo** (SPOF) es cualquier componente no replicado cuya falla interrumpe el servicio. La tabla revisa la arqui-

tectura en busca de SPOF.

Tabla 3. Análisis de puntos únicos de fallo

Componente	¿Por qué podría ser un SPOF?	Mitigación aplicada
Base de datos	Una sola instancia de SQL Server detendría los tres sistemas.	RDS Multi-AZ con réplica sincrónica y conmutación automática.
Servidores de aplicación	Una única instancia o tarea concentra todo el tráfico.	Grupo de Auto Scaling con mínimo dos instancias, una por zona.
Salida a Internet	Un solo NAT Gateway deja sin salida a ambas zonas si falla la suya.	Un NAT Gateway por zona de disponibilidad.
Conexión híbrida	Un único túnel VPN corta la replicación durante la migración.	Dos túneles VPN redundantes (los provee AWS por defecto).
Región	Toda la plataforma depende de una sola región.	Copias en otra región y procedimiento de recuperación documentado.
Personas	Un único administrador concentra el conocimiento y los accesos.	Roles compartidos, documentación, infraestructura como código y cuenta de emergencia (*break-glass*) custodiada.

Fuente: elaboración propia.

1.5 Riesgos de contenedores y de infraestructura mutable

Los contenedores permiten ejecutar una aplicación de forma idéntica en cualquier entorno, pero introducen riesgos propios:

- **Imágenes vulnerables o maliciosas** descargadas de repositorios públicos sin verificación.
- **Secretos dentro de las imágenes** (contraseñas o claves escritas en el código o en el Dockerfile).
- **Contenedores con privilegios excesivos**, que ejecutan procesos como *root* o con acceso al host.
- **Falta de orquestación y control** sobre qué versión de cada servicio está en ejecución.

Por otro lado, en una **infraestructura mutable** los servidores se modifican después de implementarse: parches manuales, cambios de configuración "en caliente". Con el tiempo, cada servidor termina siendo distinto de los demás (*configuration drift*), los errores son difíciles de reproducir y no queda claro qué cambió ni quién lo cambió. Ambos riesgos se tratan en la sección 3 con imágenes versionadas, escaneo automático e infraestructura inmutable.

1.6 Matriz consolidada de riesgos

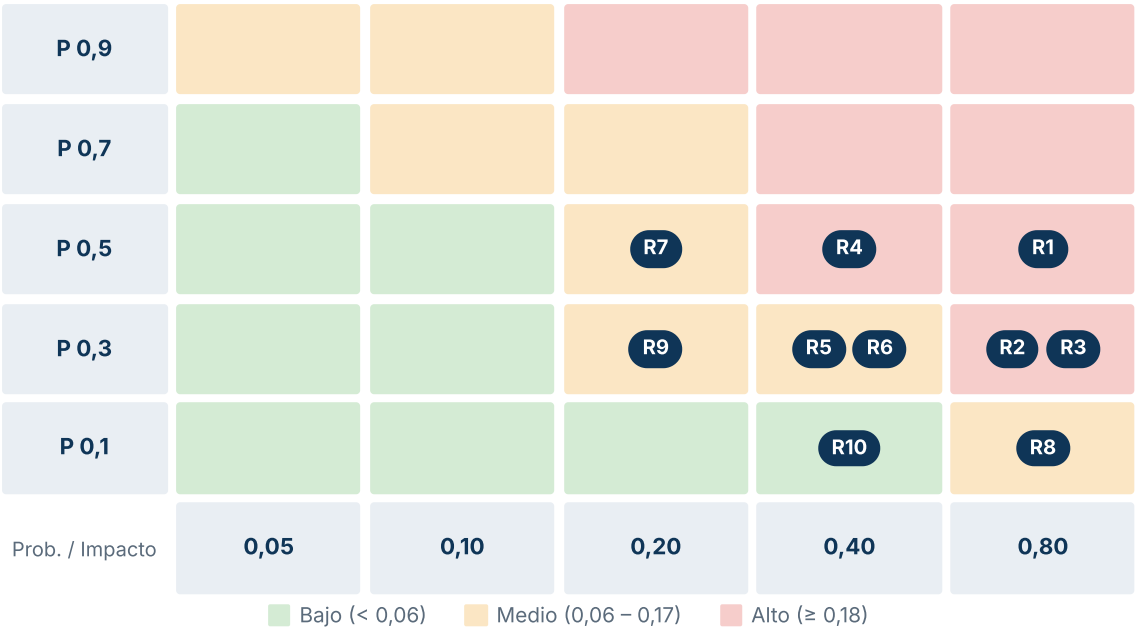
Siguiendo la metodología del Módulo 1, se estima cada riesgo con la fórmula **Riesgo = Probabilidad × Impacto**, usando las mismas escalas: bajo, menor a 0,06; medio, entre 0,06 y 0,17; alto, desde 0,18.

Tabla 4. Evaluación de riesgos de la arquitectura cloud

#	Riesgo	P	I	Nivel	Estrategia	Tratamiento principal
R1	Configuración incorrecta que expone datos o servicios	0,5	0,80	0,40 Alto	Mitigar	Infraestructura como código revisada, AWS Config y Security Hub.
R2	Credenciales comprometidas o abuso de privilegios	0,3	0,80	0,24 Alto	Mitigar	MFA, mínimo privilegio, roles temporales y alertas.
R3	Ransomware sobre bases, archivos o instancias	0,3	0,80	0,24 Alto	Mitigar	Copias inmutables en cuenta separada y pruebas de restauración.
R4	Imagen de contenedor vulnerable o con código malicioso	0,5	0,40	0,20 Alto	Mitigar	Escaneo en el pipeline y en ECR; imágenes base aprobadas.
R5	Falla de un componente único (SPOF)	0,3	0,40	0,12 Medio	Mitigar	Redundancia Multi-AZ en todas las capas.
R6	Movimiento lateral por segmentación insuficiente	0,3	0,40	0,12 Medio	Mitigar	Subredes por capa, *security groups* encadenados, Network Firewall.
R7	Deriva de configuración en servidores mutables	0,5	0,20	0,10 Medio	Evitar	Infraestructura inmutable: se reemplaza, no se modifica.
R8	Escape de máquina virtual en el hipervisor	0,1	0,80	0,08 Medio	Transferir	Responsabilidad del proveedor; certificaciones verificables en AWS Artifact.
R9	Falta de registros para investigar un incidente	0,3	0,20	0,06 Medio	Mitigar	Registros centralizados e inmutables (sección 2.3).
R10	Indisponibilidad de una región completa	0,1	0,40	0,04 Bajo	Aceptar	Copias en otra región; se acepta el tiempo de recuperación.

Fuente: elaboración propia con base en la matriz de Barato (2014). P = probabilidad; I = impacto.

Figura 1. Mapa de calor de los riesgos identificados



Fuente: elaboración propia.

Los cuatro riesgos altos tienen un rasgo común: todos dependen de decisiones de **configuración, identidades y procesos** de Tech Consulting, no del proveedor. Por eso, como se verá a continuación, la auditoría continua y la automatización propia de DevOps son las respuestas más efectivas.

2 Funcionalidades de la auditoría informática

2.1 Concepto y beneficios

La auditoría informática es un estudio profesional que realizan especialistas en ciberseguridad, generalmente ajenos a la empresa, con el objetivo de detectar las vulnerabilidades y amenazas de la tecnología que sostiene la estrategia de negocio (“Por qué es necesario hacer una auditoría de seguridad informática”, s. f.). En un entorno cloud, la auditoría verifica que los controles diseñados realmente estén funcionando y que la organización pueda demostrarlo.

Beneficio	Aplicación en Tech Consulting
Detecta debilidades en los sistemas de seguridad	Errores de código en los microservicios y configuraciones inseguras en la cuenta de AWS.
Identifica posibles actuaciones fraudulentas	Accesos no autorizados a datos comerciales o cambios de permisos sin justificación.
Mejora los controles internos	Verifica que RBAC, MFA y cifrado se apliquen igual en todos los entornos.

Beneficio	Aplicación en Tech Consulting
Elimina puntos débiles	Cada hallazgo genera una acción correctiva con responsable y fecha.
Mantiene los sistemas actualizados	Controla el nivel de parches de instancias, imágenes y dependencias.

2.2 Tipos de auditoría aplicados al caso

Tabla 5. Plan de auditorías propuesto

Tipo	Alcance en Tech Consulting	Herramientas de apoyo	Frecuencia
Web	Productos digitales y APIs expuestas a través del balanceador.	Pruebas de penetración autorizadas, OWASP ZAP, registros de AWS WAF.	Anual y ante cambios mayores.
Código fuente	Microservicios, scripts de procesamiento de datos e infraestructura como código.	SonarQube (análisis estático), revisión de dependencias, escaneo de plantillas IaC.	Continua, en cada cambio (pipeline).
Redes	VPC, *security groups*, rutas, VPN y salida a Internet.	VPC Flow Logs, AWS Config, Network Access Analyzer.	Trimestral y continua.
Dispositivos e infraestructura	Instancias, imágenes y contenedores. La infraestructura física la audita AWS.	Amazon Inspector, Systems Manager, informes SOC e ISO en AWS Artifact.	Continua; revisión semestral.
Forense	Investigación posterior a un incidente: qué pasó, cómo y qué datos se afectaron.	CloudTrail, Amazon Detective, *snapshots* de volúmenes aislados.	Ante cada incidente.

Fuente: elaboración propia con base en "Qué es una auditoría de seguridad informática: tipos y fases" (2021).

La auditoría de la infraestructura física merece una aclaración: en la nube, Tech Consulting no puede ingresar a los centros de datos de AWS. Se apoya, en cambio, en los informes de auditorías independientes que el proveedor publica (SOC 1/2/3, ISO 27001), disponibles en AWS Artifact. Es la aplicación directa del modelo de responsabilidad compartida a la auditoría.

2.3 Registros de auditoría en la nube

Sin registros no hay auditoría posible. Se propone registrar, centralizar y proteger las siguientes fuentes:

Tabla 6. Registros de auditoría propuestos

Registro	Qué responde	Retención sugerida
AWS CloudTrail	¿Quién hizo qué acción sobre la cuenta, cuándo y desde dónde?	Al menos 1 año
Eventos de datos de S3	¿Quién leyó, modificó o borró cada objeto del data lake?	1 año

Registro	Qué responde	Retención sugerida
VPC Flow Logs	¿Qué tráfico se aceptó o rechazó entre subredes y hacia Internet?	90 días
Auditoría de SQL Server (RDS)	¿Quién consultó o modificó datos sensibles en las bases transaccionales?	1 año
Registros del ALB y de AWS WAF	¿Qué solicitudes recibieron los productos digitales y cuáles se bloquearon?	90 días
Registros de contenedores e instancias	¿Qué hizo cada aplicación y qué errores generó?	30 a 90 días
Historial de AWS Config	¿Cómo estaba configurado cada recurso en una fecha dada?	1 año

Fuente: elaboración propia. Los plazos son orientativos y deben ajustarse a la normativa aplicable.

> **PROTECCIÓN DE LOS REGISTROS**
>
> Los registros se envían a una **cuenta de archivo separada**, a la que los administradores de producción no tienen acceso de escritura. Se almacenan en S3 con cifrado, **Object Lock** (no se pueden borrar ni modificar durante el período de retención) y la validación de integridad de CloudTrail activada. Así, aun si un atacante obtiene privilegios en producción, no puede borrar sus huellas.

2.4 Funcionalidades y proceso de auditoría

Integrando lo anterior, la auditoría informática aporta cinco funcionalidades a la plataforma de Tech Consulting:

FUNCIONALIDAD 1

Trazabilidad

Reconstruir cualquier acción sobre la cuenta, la red o los datos, con usuario, hora y origen.

FUNCIONALIDAD 2

Detección

Identificar accesos indebidos, configuraciones inseguras y comportamientos anómalos.

FUNCIONALIDAD 3

Control continuo

Evaluar en forma automática el cumplimiento de reglas con AWS Config, Security Hub y AWS Audit Manager.

FUNCIONALIDAD 4

Evidencia y cumplimiento

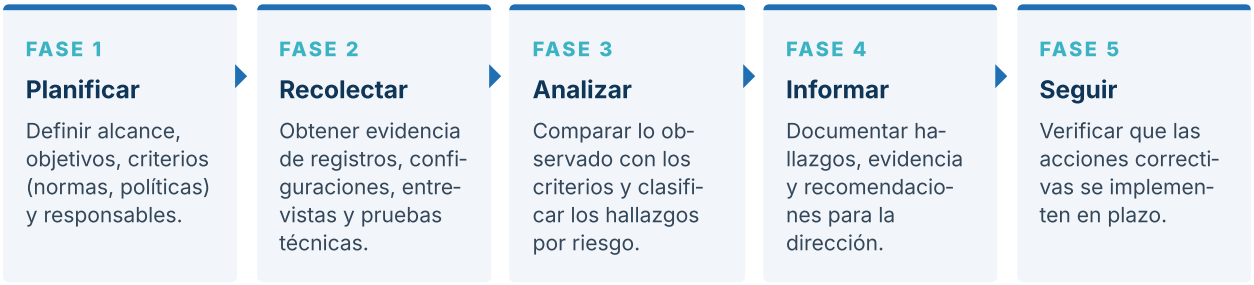
Demostrar ante terceros el tratamiento adecuado de los datos personales, conforme a la Ley 25.326.

FUNCIONALIDAD 5

Investigación forense y mejora

Ante un incidente, determinar causa, alcance y datos afectados, y convertir las conclusiones en nuevos controles.

Figura 2. Fases del proceso de auditoría



Fuente: elaboración propia.

3 Beneficios de la integración DevOps + Cloud

3.1 Qué es y qué no es DevOps

DevOps —contracción de *Development* y *Operations*— es una cultura que busca mejorar la agilidad en la entrega de servicios de TI mediante la comunicación transparente, la colaboración y la integración entre desarrollo y operaciones, desde la planificación y el diseño del software hasta su despliegue en producción ("DevOps, el nuevo lenguaje entre áreas de desarrollo y operaciones", s. f.). Se resume en tres componentes: **colaboración + procesos + herramientas**.

Es tan importante entender qué **no** es: no es sólo automatización, no es sólo usar servicios cloud, no es una herramienta que se instala y no es un equipo nuevo aislado del resto de TI. Para Tech Consulting esto significa que adoptar DevOps implica cambiar la forma de trabajar entre quienes desarrollan los productos digitales, quienes operan la plataforma y quienes la protegen. Cuando la seguridad se integra en ese ciclo desde el inicio se habla de **DevSecOps**.

3.2 Pipeline CI/CD propuesto

El núcleo técnico de DevOps es la automatización del ciclo de entrega:

- **Integración continua (CI):** los desarrolladores integran su código a un repositorio común varias veces al día; cada integración se compila y se prueba automáticamente.
- **Entrega continua (CD):** el software queda siempre listo para desplegarse; el pase a producción requiere una aprobación humana.

- **Despliegue continuo:** el pase a producción es totalmente automático y sólo una prueba fallida lo detiene.

Para Tech Consulting se propone comenzar con **entrega continua** (con aprobación manual antes de producción) y evolucionar a despliegue continuo para los microservicios de menor criticidad una vez que las pruebas automáticas sean confiables.

Figura 3. Pipeline DevSecOps propuesto para los microservicios



Fuente: elaboración propia. En rojo, las etapas de control de seguridad; en turquesa, las de operación.

3.3 Contenedores, orquestación e infraestructura inmutable

Docker automatiza la implementación de aplicaciones como contenedores portátiles y autosuficientes que pueden ejecutarse en la nube o localmente. Aporta modularidad, capas y control de versiones de imágenes, implementación rápida y restauración de versiones anteriores. Los microservicios de Tech Consulting se empaquetan como imágenes Docker y se almacenan, versionadas, en Amazon ECR.

Para administrarlos se requiere un **orquestador**. Kubernetes es el estándar de la industria y organiza los contenedores en *pods*, *nodos* y *clústeres* bajo un plano de control. En la propuesta se usa **Amazon ECS sobre Fargate**, un orquestador gestionado más simple de operar; si en el futuro la empresa necesitara portabilidad entre proveedores, podría migrar a **Amazon EKS** (Kubernetes gestionado) sin cambiar las imágenes.

Finalmente, se adopta la **infraestructura inmutable**: los servidores y contenedores nunca se modifican después de implementarse. Si algo necesita actualizarse, se construye una nueva imagen (con EC2 Image Builder para las AMI o con el pipeline para los contenedores), se valida y reemplaza a la anterior, que se retira.

Aspecto	Infraestructura mutable (actual)	Infraestructura inmutable (propuesta)
Actualizaciones	Parches y cambios sobre el servidor en ejecución.	Se reemplaza el servidor por uno nuevo a partir de una imagen actualizada.
Consistencia	Cada servidor diverge con el tiempo (deriva de configuración).	Todos los entornos son idénticos: desarrollo, prueba y producción.
Vuelta atrás	Difícil: hay que deshacer cambios manuales.	Inmediata: se vuelve a desplegar la imagen anterior.
Seguridad	Un atacante puede persistir en un servidor de larga vida.	Los servidores se renuevan con frecuencia, lo que elimina persistencias.
Auditoría	Cambios difíciles de rastrear.	Cada versión está registrada en el repositorio y en el pipeline.

Fuente: elaboración propia con base en Alvarado (2021).

3.4 Beneficios para Tech Consulting

El módulo enumera siete beneficios de implementar una cultura DevOps. La tabla los vincula con los problemas del escenario y con los riesgos de la sección 1.

Tabla 7. Beneficios de DevOps + Cloud aplicados al caso

Beneficio	Cómo se concreta en Tech Consulting	Riesgo o problema que reduce
Mejora la comunicación	Desarrollo, operaciones y seguridad comparten repositorio, pipeline y paneles de monitoreo.	Silos entre áreas; métricas con criterios propios.
Escalabilidad en los servicios	Contenedores e infraestructura como código permiten replicar y escalar servicios en minutos.	Demanda creciente de productos digitales.
Mayor seguridad	Controles automáticos en cada cambio, imágenes escaneadas y configuraciones revisadas antes de llegar a producción.	R1, R4, R7.
Reducción de costos	Menos trabajo manual, menos incidentes y entornos de prueba que se crean y destruyen bajo demanda.	Capacidad ociosa y retrabajo.
Seguimiento continuado	El monitoreo de CloudWatch y los registros de auditoría forman parte del ciclo.	R9; detección tardía de fallas.
Publicaciones más frecuentes	Cambios pequeños y frecuentes, más fáciles de probar y de revertir.	Despliegues grandes y riesgosos.
Software de mejor calidad	Pruebas automáticas y análisis de código en cada integración.	Errores de programación que llegan a producción.

Fuente: elaboración propia con base en los contenidos del módulo.

La combinación con la nube es lo que hace posibles estos beneficios: sin infraestructura programable y bajo demanda, no se podrían crear entornos idénticos en minutos, reemplazar servidores en lugar de parchearlos ni escalar en forma automática. DevOps aporta el *cómo trabajar*, y la nube, el *dónde* hacerlo con elasticidad.

3.5 Cómo medir los beneficios

Para verificar que la adopción de DevOps funcione, se proponen las cuatro métricas del programa de investigación DORA (Forsgren et al., 2018), ampliamente utilizadas en la industria:

Frecuencia de despliegue: cuántas veces se publica a producción por semana.	**Lead time** tiempo desde que un cambio se integra hasta que llega a producción.	**Tasa de fallo** porcentaje de cambios que provocan incidentes o requieren vuelta atrás.
MTTR tiempo medio para restaurar el servicio tras una falla.	**Hallazgos** vulnerabilidades críticas detectadas en el pipeline antes de producción.	**Cumplimiento** porcentaje de recursos que cumplen las reglas de AWS Config.

Fuente: elaboración propia con base en Forsgren et al. (2018). Las dos últimas son métricas de seguridad complementarias.

4 Conclusiones

El análisis de riesgos muestra que la arquitectura cloud de Tech Consulting está bien protegida en las capas que gestiona el proveedor —hardware, hipervisor, centros de datos—, pero que los **riesgos más altos se ubican del lado de la empresa**: configuraciones incorrectas, credenciales comprometidas, *ransomware* e imágenes de contenedor vulnerables. La segmentación de red, la eliminación de puntos únicos de fallo y las copias inmutables reducen esos riesgos, pero sólo si se aplican y se mantienen de forma consistente.

Ahí aparece el valor de la **auditoría informática**. Con registros centralizados e inalterables, un plan que combina auditorías web, de código, de redes, de infraestructura y forenses, y controles automáticos continuos, la organización puede verificar que sus controles funcionan, detectar desvíos a tiempo y demostrar el cumplimiento de sus obligaciones de protección de datos.

Por último, la **integración DevOps + Cloud** transforma la seguridad de una revisión puntual en una práctica cotidiana. Un pipeline CI/CD con controles de seguridad, contenedores versionados e infraestructura inmutable hace que cada cambio sea pequeño, probado, trazable y reversible. Así se atacan en su origen varios de los riesgos identificados, al tiempo que se obtienen los beneficios de negocio buscados desde la Actividad 1: escalabilidad, calidad, menor costo operativo y capacidad de responder a una demanda creciente.

En síntesis, riesgos, auditoría y DevOps no son temas aislados, sino un ciclo: se identifican los riesgos, se automatizan los controles en el pipeline, se audita su cumplimiento y lo aprendido vuelve a alimentar la gestión de riesgos.

5 Referencias bibliográficas

Alvarado, G. (2021). *Beneficios y retos de la infraestructura inmutable + Tutorial: Packer, Ansible y Terraform*. https://galvarado.com.mx/post/beneficios-retos-y-como-lograr-infraestructura-inmutable-con-packer-ansible-y-terraform/

Amazon Web Services. (s. f.-a). *Modelo de responsabilidad compartida*. https://aws.amazon.com/es/compliance/shared-responsibility-model/

Amazon Web Services. (s. f.-b). *AWS CloudTrail: Guía del usuario*. https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/

Amazon Web Services. (s. f.-c). *AWS Artifact*. https://aws.amazon.com/es/artifact/

Barato, J. (2014). *Gestión eficaz de los riesgos del proyecto*. http://jose-barato.blogspot.com/2014/04/gestion-eficaz-de-los-riesgos-del.html

Bejerano, P. (2017). *¿Para qué sirven los contenedores en software?* Think Big. https://blogthinkbig.com/para-que-sirven-los-contenedores-en-software

DevOps, el nuevo lenguaje entre áreas de desarrollo y operaciones. (s. f.). *World EADAIT*. https://worldaedait.com.mx/devops-el-nuevo-lenguaje-entre-areas-de-desarrollo-y-operaciones/

Forsgren, N., Humble, J. y Kim, G. (2018). *Accelerate: The science of lean software and DevOps*. IT Revolution Press.

Hipervisor: el medio para la virtualización. (2020). *IONOS Digital Guide*. https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-hypervisor/

Información sobre Docker. (2022). *Microsoft*. https://docs.microsoft.com/es-es/dotnet/architecture/containerized-lifecycle/what-is-docker

Integración continua y entrega continua. (s. f.). *Aplyca*. https://www.aplyca.com/es/blog/integracion-continua-y-entrega-continua-cicd

Kubernetes: ventajas del gestor de contenedores. (2019). *IONOS Digital Guide*. https://www.ionos.es/digitalguide/servidores/know-how/que-es-kubernetes/

Ley 25.326 de Protección de los Datos Personales. (2000). Boletín Oficial de la República Argentina.

López, A. (2019). *¿Qué es seguridad informática? Segmentación de redes de datos*. LinkedIn. https://www.linkedin.com/pulse/qu%C3%A9-es-seguridad-inform%C3%A1tica-segmentaci%C3%B3n-de-redes-datos-arturo-lopez

Por qué es necesario hacer una auditoría de seguridad informática. (s. f.). *Blog de Seguridad para Empresas*. https://uss.com.ar/corporativo/auditoria-de-seguridad-informatica/

¿Qué es la segmentación de la red? (s. f.). *Palo Alto Networks*. https://www.paloaltonetworks.es/cyberpedia/what-is-network-segmentation

¿Qué es un malware?: Tipos y maneras de evitar ataques de este tipo. (2021). *Red Seguridad*. https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html

Qué es una auditoría de seguridad informática: tipos y fases. (2021). *Ambit*. https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases

SPOF Single Point Of Failure o punto simple de fallo. (s. f.). *HispaLinux*. https://www.ibiblio.org/pub/linux/docs/LuCaS/Presentaciones/200103hispalinux/paredes/html/x27.html

TECLAB Instituto Técnico Superior. (s. f.). *Seguridad en la Nube y Protección de Datos: Módulo 3. Virtualización y contenedores* [Material de cátedra].